Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет «Комп'ютерні технології і системи»
(назва факультету)

Кафедра «Електронні обчислювальні машини»
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(ступінь вищої освіти)

на тему: Розробка засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком

за освітньою програмою Кібербезпека
зі спеціальності: 125 Кібербезпека
(шифр і назва спеціальності)

Виконав: студент групи: КБ1811

	(підпис студента)	/ Данило ЯРЬОМЕНКО / (Ім`я ПРІЗВИЩЕ)
Керівник:	(підпис)	/ доцент, Денис ОСТАПЕЦЬ / (посада, Ім`я ПРІЗВИЩЕ)
Нормоконтролер:	(підпис)	/ ст. викладач, Володимир ДЗЮБА / (посада, Ім`я ПРІЗВИЩЕ)

Консультанти:

(назва розділу)	(підпис)	/ / (посада, Ім`я ПРІЗВИЩЕ)
(назва розділу)	(підпис)	/ / (посада, Ім`я ПРІЗВИЩЕ)
(назва розділу)	(підпис)	/ / (посада, Ім`я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Дніпро –2022 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Faculty «Computer technologies and systems»
(faculty)

Department «Electronic computers»
(department)

Explanatory Note
to Bachelor's Thesis
bachelor's
(higher education degree)

on the topic: Development of means for demonstrating biometric identification and authentication by keyboard handwriting

in the Speciality: 125 Cybersecurity
(speciality and its code)

Done by the student of the group: KB1811 / Danylo Yaromenko /
(name, surname)

Scientific Supervisor: / Associate Professor, Denis Ostapets /
(position, name, surname)

Normative controller : / Senior lecturer, Volodymyr Dziuba /
(position, name, surname)

Supervisors

(Chapter title heading)	/ (position, name, surname)
(Chapter title heading)	/ (position, name, surname)
(Chapter title heading)	/ (position, name, surname)
(Chapter title heading)	/ (position, name, surname)

Dnipro – 2022

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: ЕОМ
Рівень вищої освіти: Перший (бакалаврський)
Освітня програма: Кібербезпека
Спеціальність: 125 Кібербезпека
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри _____
_____ _____
(підпис) (Ім'я ПРІЗВИЩЕ)
Дата _____

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра
(ступінь вищої освіти)

студенту Ярьоменку Данилу Олександровичу
(Прізвище, Ім'я По батькові)

1. Тема роботи: Розробка засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком

Керівник роботи: Остапець Денис Олександрович, к.т.н., доцент
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "07" 12 2021 р. № 67ст

2. Строк подання студентом роботи: 13.06.2022 р.
3. Вихідні дані до роботи:
Методи та алгоритми біометричної ідентифікації та аутентифікації за клавіатурним почерком
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):
4.1 Аналітична частина:
Аналіз методів біометричної ідентифікації та аутентифікації за клавіатурним почерком
4.2 Основна частина:
- Огляд та аналіз методів та засобів біометричної ідентифікації та аутентифікації;
- Організація розроблювальних засобів;
- Розробка програмного забезпечення.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
- Характеристики біометричних методик;
- Характеристики алгоритмів розпізнавання клавіатурного почерку;
- Організація та функції комплексу;
- Структура даних;
- Основні алгоритми програми;

- Приклади роботи комплексу.

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв: (підпис студента, дата)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд та аналіз методів та засобів біометричної ідентифікації та аутентифікації	25.04.22	20%
2	Організація розроблювальних засобів	12.05.22	25%
3	Розробка та налагодження програмного забезпечення	06.06.22	50%
4	Реферат, вступ, висновки	13.06.22	5%
5	Подання кваліфікаційної роботи до кафедри	13.06.22	
6	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.06.22	

Студент _____ (підпис) Данило ЯРЬОМЕНКО (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Денис ОСТАПЕЦЬ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи бакалавра:

60 с., 24 рис., 5 табл., 6 додатків, 7 джерел.

Об'єкт розробки – програмні засоби демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком.

Мета роботи – розробка програмних засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком під час введення текстового фрагменту.

Представлено аналіз біометричних методів ідентифікації, алгоритмів розпізнавання за клавіатурним почерком. Обрано метод біометричної ідентифікації та аутентифікації за клавіатурним почерком під час введення текстового фрагменту. Наведені узагальнені алгоритми роботи засобів в різних режимах, розроблено програмне забезпечення засобів та перевірена його працездатність, створено інструкцію з використання.

Розроблене програмне забезпечення може використовуватися для демонстрації процесу ідентифікації та аутентифікації за клавіатурним почерком та у навчальному процесі.

Ключові слова: БІОМЕТРІЯ, АУТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, КЛАВІАТУРНИЙ ПОЧЕРК, СТАТИСТИЧНІ ДАНІ, БІОМЕТРИЧНІ ХАРАКТЕРИСТИКИ, C++

ЗМІСТ

ВСТУП

В сучасному світі гостро стоїть проблема конфіденційності, всі люди мають інформацію, що вимагає збереження та особливих умов доступу до неї. Саме механізми аутентифікації та ідентифікації вирішують проблеми конфіденційного доступу до інформації.

Біометричні системи ідентифікації та аутентифікації, безумовно, складні у реалізації та їх можливості зараз дуже обмежені через недосконаліть апаратних засобів та математичних моделей. Але враховуючи регулярний прогрес (збільшення обчислювальної потужності, розвиток математичних моделей, вивчення нейросетевих технологій), біометричні системи можуть значно потіснити системи інших типів. Важливу роль грає зручність використання системи користувачами, що також виділяє біометричні системи. Впровадження зручних для користувачів систем біометричної ідентифікації та аутентифікації – це насущне питання, тому тема роботи є актуальною.

Тема роботи затверджена наказом № 67 ст від 07.12.2021.

Мета роботи – розробка програмних засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком під час введення текстового фрагменту.

Основні положення даної роботи доповідались та були схвалені на XV Міжнародній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» у 2021 році (див. додаток А).

Робота складається із вступу, трьох розділів та висновків.

1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

1.1 Загальні відомості та поняття біометрії

Будь хто може пройти аутентифікацію за володінням якоюсь річчю, за знанням якоїсь інформації або за набором фізіологічних показників – це простий опис трьох факторів аутентифікації: майнового, парольного та біометричного відповідно [1], класифікацію факторів аутентифікації наведено на рисунку 1.1.

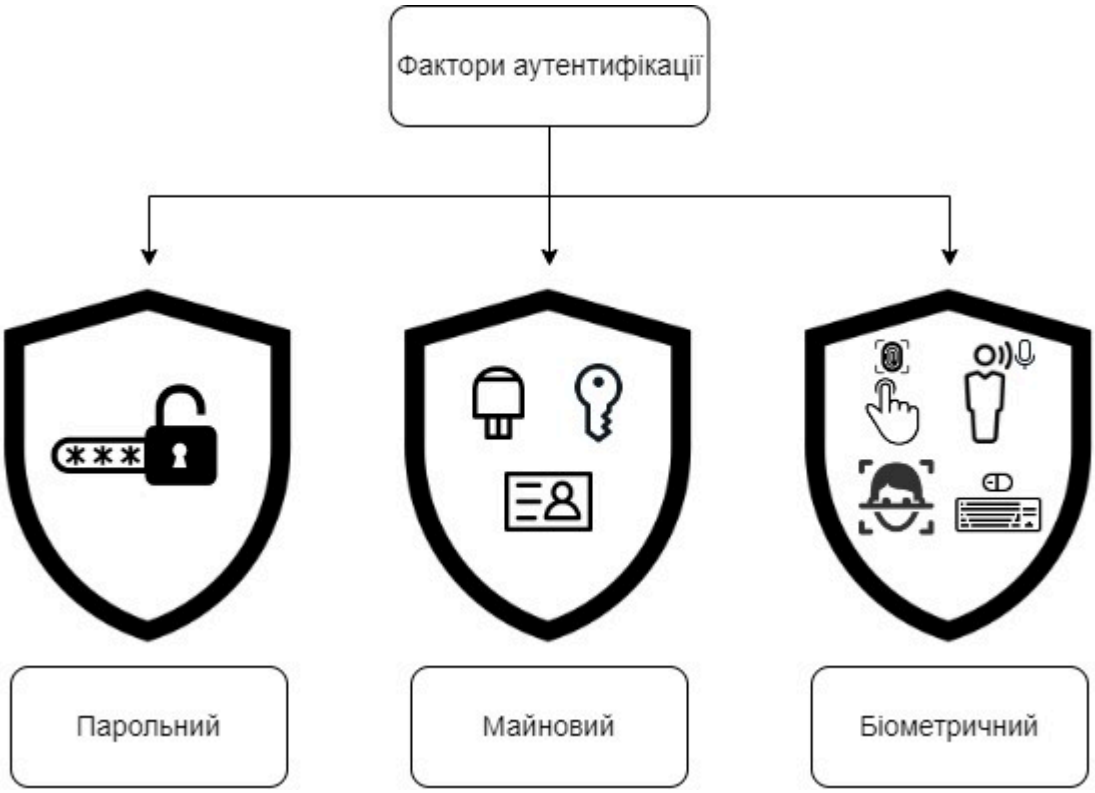


Рисунок 1.1 – Фактори аутентифікації

Річ – це фізичний об’єкт, яким людина може скористуватись, щоб пройти процедуру аутентифікації. Це можуть бути картки пропуску, ключи, id-картки тощо.

Інформація, в контексті фактору аутентифікації – це паролі, коди, відповіді на контрольні запитання тощо.

Фізіологічні показники – це унікальні характеристики, притаманні будь-який людині.

Найбільш розповсюджений фактор аутентифікації на сьогоднішній день – фактор знання. Аутентифікація не потребує ніяких додаткових витрат, лише запам'ятовування секретної інформації. Людина постійно стикається з цим фактором аутентифікації, коли реєструється на будь-яких сайтах в мережі Internet. Другим за розповсюдженістю є фактор володіння, який набирає все більшої популярності, зокрема в Україні, в зв'язку з малим ступенем захищеності за допомогою паролів, PIN-кодів тощо, та удосконаленням Закону «Про електронні довірчі послуги» [2]. Біометричний фактор широко розповсюджений в якості відбитків пальців, які використовуються для видачі id-карт для громадян України. Деякі стратегічні об’єкти, наприклад прикордонні КПП, також використовують системи аутентифікації за біометричним фактором. Багато компаній впроваджує на своїх об’єктах системи контролю доступу з використанням біометричних систем аутентифікації та ідентифікації. Смарт-картки – найпоширеніший спосіб, за ними співробітники, наприклад, реєструються під час прибуття або відбуття на об’єкт.

1.2 Класифікація методів аутентифікації

Біометричні методи аутентифікації на сьогоднішній день прийнято поділяти на два класи [3], класифікацію наведено на рисунку 1.2:

– статичні методи
– динамічні методи

Статичні методи засновані на фізіологічних показниках людини, які природно незмінні протягом всього його життя і їх практично неможливо вкрасти або підробити.

Динамічні методи засновані на поведінкових показниках людини, які залежать від поточного стану людини та можуть змінюватись під впливом деяких факторів.

Таким чином до статичних методів можна віднести, наприклад, аутентифікацію по відбитку пальцю, аутентифікацію по оболонці ока, аутентифікацію по геометрії обличчя. До динамічних методів відносяться:

аутентифікація за голосом, аутентифікація за почерком (рукописним або клавіатурним).

Рисунок 1.2 – Класифікація біометричних методів аутентифікації

Слід зазначити, що статичні методи аутентифікації визначають людину в багатьох випадках більш точніше, ніж динамічні, але в свою чергу потребують більш дорогого обладнання, як наприклад сканер сітчатки ока.

1.3 Характеристика динамічних методів біометричної аутентифікації

Для методів цього класу характерна більш легка реалізація, аніж реалізація біометричних систем за статичними методами, але водночас динамічні біометричні методи не дають такої точності, як статичні біометричні методи. Характеристику динамічних біометричних методів наведено в таблиці 1.1 [4].

Таблиця 1.1 – Характеристики динамічних біометричних методів

Хар-ки методу / Мет. аутент.	Відносна складність реалізації	Відносна собівартість	Відносна точність
За голосом	середня	середня	середня
За клавіатурним почерком	середня	низька	низька
За підписом	складна	висока	середня
За динамікою роботи з комп'ютерною мишею	складна	середня	середня

Огляд характеристик проводився з урахуванням можливості розробки прототипів засобів біометричної ідентифікації та аутентифікації.

1.4 Аналіз методу аутентифікації за клавіатурним почерком

Для методу розпізнавання клавіатурного почерку характерно наявність режиму навчання. Користувач може пройти аутентифікацію, після чого набрати який-небудь текст. Програма зчитує динамічні характеристики користувача і зберігає їх. Отже, після навчання в системі накопичуються дані про час утримання клавіш і паузах між натисканнями для кожного відомого користувача.

Існує три способи розпізнавання клавіатурного почерку, аналіз алгоритмів наведено в таблиці 1.2:

- фіксація вихідних даних під час введення парольної послідовності
- фіксація вихідних даних під час введення тексту
- прихована фіксація вихідних даних під час роботи користувача

Таблиця 1.2 – Характеристики алгоритмів аналізу клавіатурного почерку

Алгоритм / Хар-ки алгоритму	Фіксація вихідних даних під час введення паролю	Фіксація вихідних даних під час введення текстового фрагмента	Фіксація вихідних даних під час прихованого моніторингу
Відносна вимогливість до обчислювальної потужності	низька	низька	велика
Відносна точність	низька	середня	висока
Відносна складність реалізації	низька	низька	висока

Перший спосіб реалізації розпізнавання клавіатурного почерку має перевагу в швидкодії, бо вводиться лише фіксований пароль, який знає користувач. В такому випадку точність розпізнання, яка до того ж залежить від довжини паролю – невисока.

Другий спосіб реалізації розпізнавання клавіатурного почерку має перевагу над першим способом в точності, але користувач повинен вводити фрагменти тексту в залежності від того, що створює незручності у використанні системи.

Третій спосіб реалізації розпізнавання клавіатурного почерку має ще більшу перевагу в точності над вищезазначеними, але задля постійного прихованого моніторингу потрібні відносно великі обчислювальні потужності, особливо якщо використовується складна математична модель обробки статистичних даних (що частково вирішується шляхом періодичного прихованого моніторингу).

Розроблювальні засоби ідентифікації та аутентифікації базуються на алгоритмах другої групи.

Слід враховувати, що всі зазначені способи розпізнавання клавіатурного почерку ефективні тільки тоді, коли у користувача сформований клавіатурний почерк. Користувачі без сформованого клавіатурного почерку мають занадто

великий розкид за характеристиками, що ускладнює ідентифікацію та аутентифікацію.

Після етапу навчання комплексу слід другий етап: ідентифікація або аутентифікація. На цьому етапі в системі накопичено достатньо даних про клавіатурних почерках співробітників організації, так що можливо використовувати ці відомості для підвищення надійності аутентифікації.

Порівняння характеристик клавіатурного почерку може відбуватися з використанням ймовірносно-статистичних методів і за допомогою нейронних мереж. Вважається, що методи, засновані на застосуванні нейронних мереж, можуть забезпечити більш високу точність. При цьому вони вимагають великої обчислювальної потужності. Також можливі дві додаткові проблеми. Перша полягає в тому, що навчання такої системи може дещо затягнутися. Друга виникає через неможливість надати системі навчальну вибірку для всіх «чужих» користувачів. Ймовірносно-статистичні методи припускають підрахунок математичного очікування вибірки, а також подальше порівняння отриманих значень динамічних характеристик з еталонними для заявленого користувача [5].

Одним із способів підвищення точності роботи алгоритму є постійне оновлення еталона для користувача, який був успішно аутентифікований. Це дозволить еталону не застаріти і завжди відповідати поточним характеристикам друку користувача.

1.5 Висновки за розділом

Розглянуті основні поняття біометрії, проведено аналіз основних біометричних методів та алгоритмів розпізнавання клавіатурного почерку.

2 ОРГАНІЗАЦІЯ РОЗРОБЛЮВАЛЬНИХ ЗАСОБІВ

2.1 Склад розроблювальних засобів

Засоби, що розробляються, складаються з трьох умовних модулів: створення еталону, аутентифікація та ідентифікація. Постановку задачі наведено в додатку Л. Функціонування засобів наведено на рисунку 2.1.

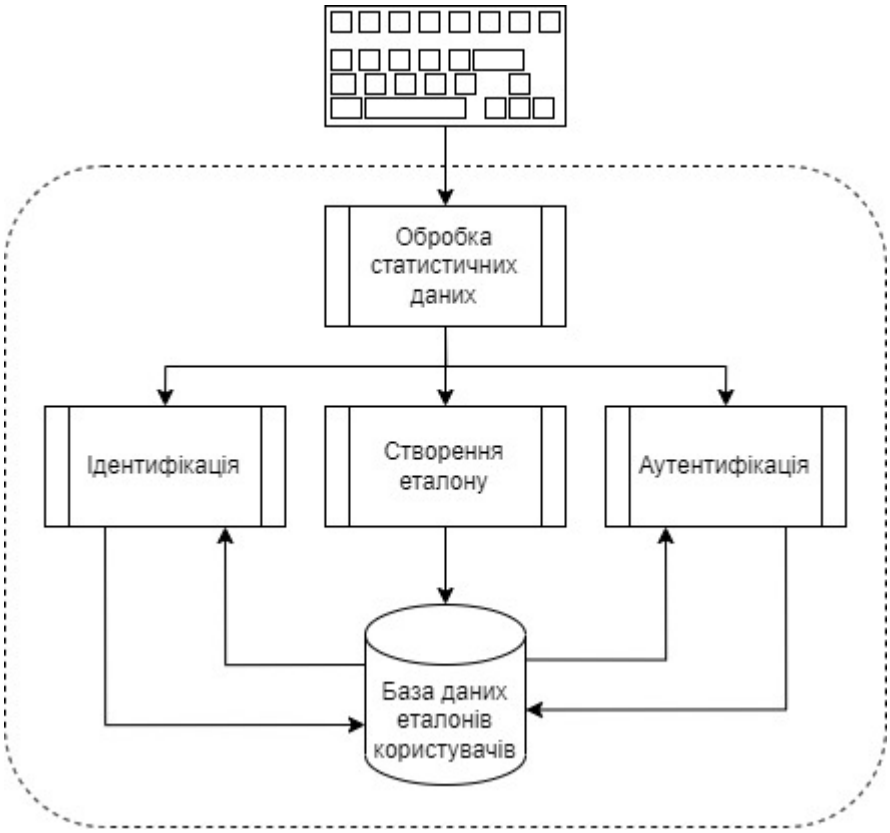


Рисунок 2.1 – Функціонування розроблюваних засобів

Модуль створення еталону оброблює вихідні дані користувача (час утримання клавіши, та інтервал між натисканням клавіш), отримуючи в результаті граничні значення, які будуть зберігатися в базі даних.

Модуль аутентифікації оброблює вихідні дані заявленого користувача та зіставляє отримані поточні характеристики з еталонними, отримуючи в результаті повідомлення про вдалу або невдалу спробу аутентифікації.

Модуль ідентифікації оброблює вихідні дані користувача та зіставляє отримані поточні характеристики з кожним еталоном в базі даних, отримуючи в результаті повідомлення про те, якому користувачу притаманний заявлений ідентифікатор.

Розробка засобів проводиться з метою демонстрації роботи, тому в базі даних користувачів буде записано вихідні дані та всі характеристики на кожному етапі обробки.

2.2 Математична модель обробки статистичних даних

Основним критерієм відповідності характеристики заявленого користувача її еталону буде влучання в межі математичного очікування для даної характеристики.

У якості вихідних даних використовується значення часу в мс, що буде фіксуватися під час натискання клавіши та відпускання клавіши, отримуючи таким чином час утримання клавіши та інтервал часу між натисканням клавіш, які будуть використані при обчисленні характеристик. Приклад вихідних даних наведено на рисунку 2.2

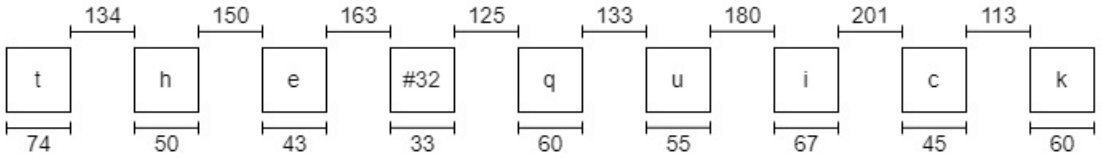


Рисунок 2.2 – Приклад набору вихідних даних для обчислення характеристик клавіатурного почерку користувача

При отриманні вихідних даних, обчислюється середнє значення кожної характеристики за формулою [6]:

$$m_j(s_j) = \frac{(j-1)\times m_{j-1}(s_j)+s_j}{j} \quad (2.1)$$

де $m_j(s_j)$ – середнє значення характеристики s після j-й ітерації натискання відповідної клавіши;

s_j – значення характеристики при j-й ітерації натисканні відповідної клавіши.

Для кожного середнього значення характеристики обчислюється середнє відхилення за формулою [6]:

$$\sigma_j(s_j) = \sqrt{\frac{(j-2)\sigma^2{}_{j-1}(s_j)+(s_j-m_j(s_j))^2}{j-1}} \quad (2.2)$$

де $\sigma_j(s_j)$ – середнє відхилення характеристики s після j-й ітерації натискання відповідної клавіши.

Визначаються межі відхилення характеристики за формулами [6]:

$$min_j(s_j) = m_j(s_j) - k \times \sigma(s_j) \quad (2.3)$$

$$max_j(s_j) = m_j(s_j) + k \times \sigma(s_j) \quad (2.4)$$

де $min_j(s_j)$ – нижня границя відхилення характеристики s після j-й ітерації натискання відповідної клавіши;

$max_j(s_j)$ – верхня границя відхилення характеристики s після j-й ітерації натискання відповідної клавіши;

k – коефіцієнт масштабування.

2.3 Інформаційна структура

Про кожного користувача в базі даних зберігається інформація (еталон). Для зручності пропонується структура зберігання характеристик користувача яка наведена на рисунку 2.3 – таке представлення даних полегшить доступ до них як з боку засобів ідентифікації та аутентифікації, так і з боку користувача в цілях демонстрації та ознайомлення з процесами механізму ідентифікації та аутентифікації на кожному етапі. Приклад реалізації структури зберігання еталону користувача в файлах з розширенням txt наведено на рисунку 2.4.

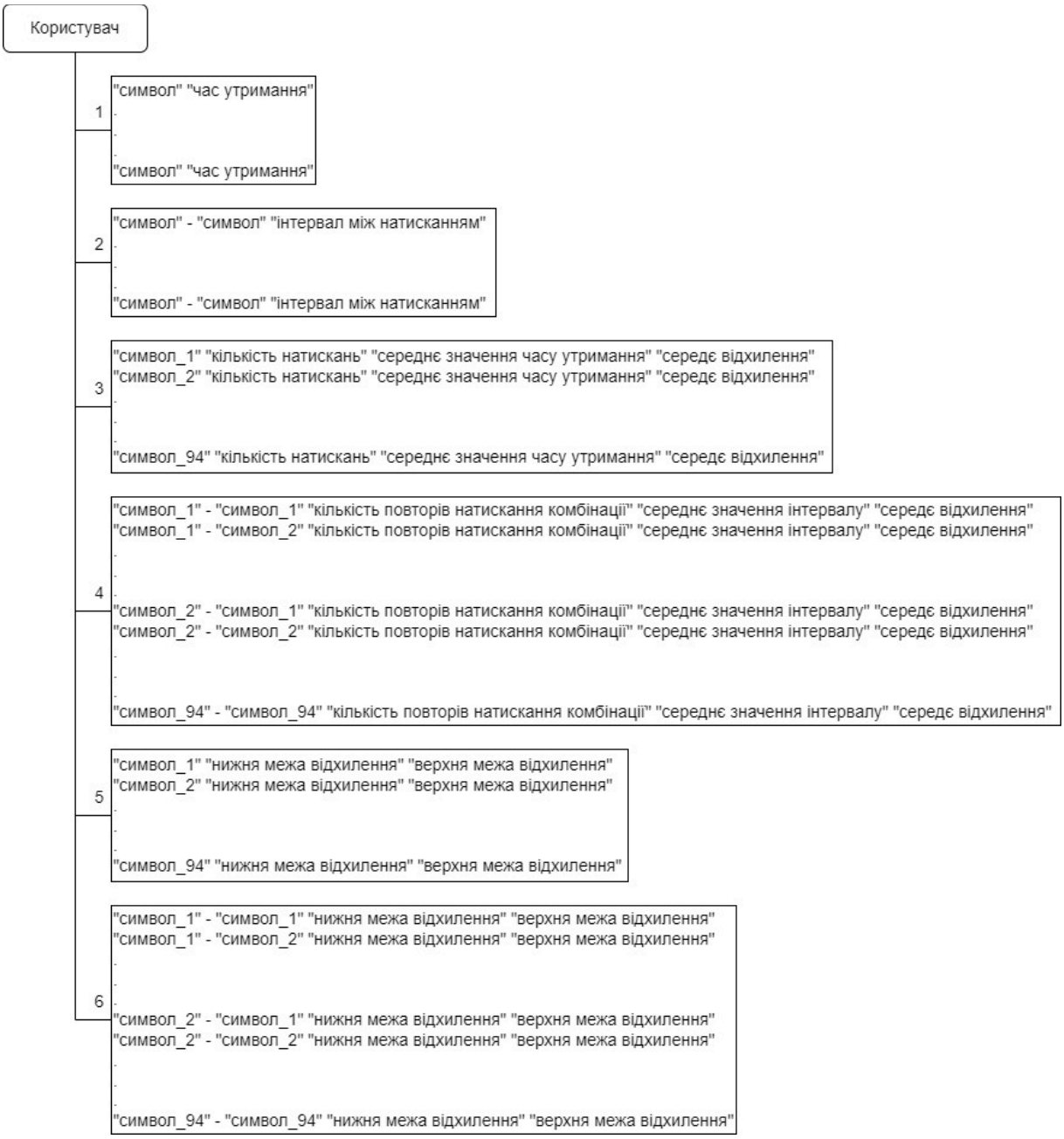


Рисунок 2.3 – Структура записів для зберігання характеристик користувача

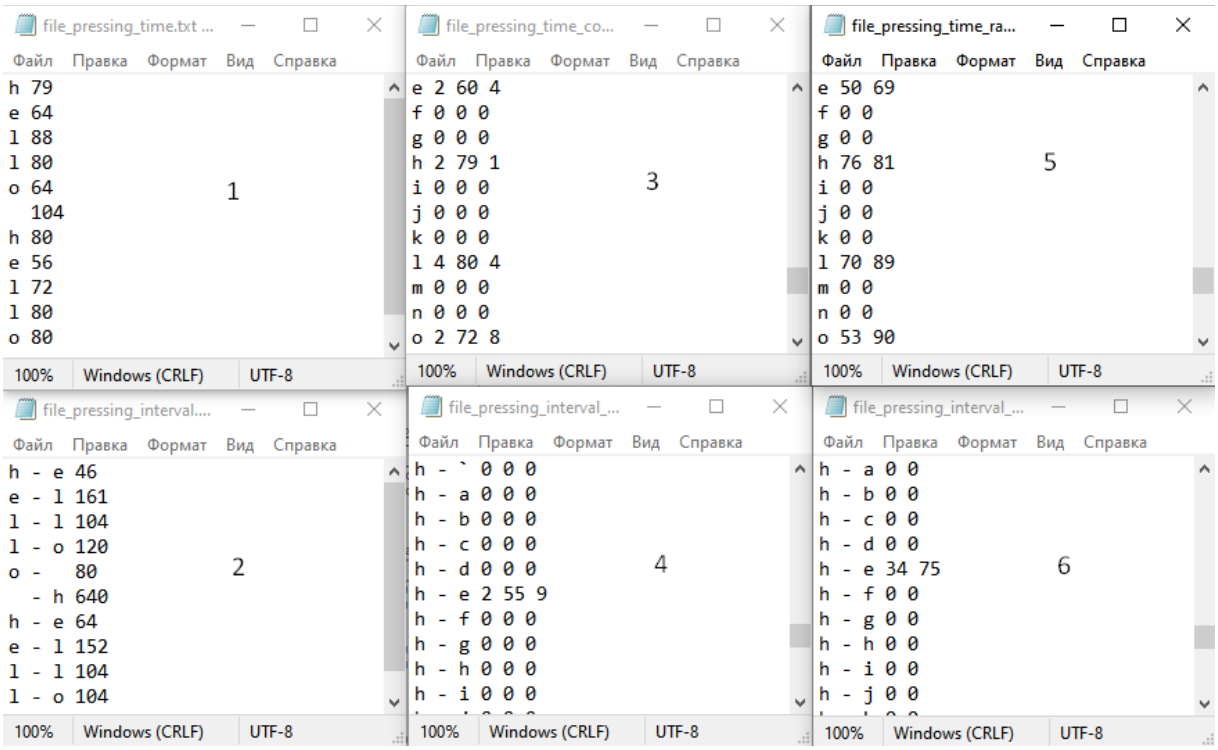


Рисунок 2.4 – Збереження характеристик користувача в файлах формату «txt»

2.4 Висновки за розділом

Представлено функціонування розроблювальних засобів, створена математична модель та інформаційна структура.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Вибір засобів реалізації

Для реалізації засобів демонстрації біометричної аутентифікації та ідентифікації обрано середовище розробки Visual Studio 2019 з фреймворком .NET (ver. 4.6.1), мова програмування C++ (стандарт – C++17 [7]).

Середовище розробки Visual Studio 2019 обрано автором за такими критеріями:

- основне середовище для роботи з C-подібними мовами.
- зручний інтерфейс
- можливість налагодження (дебаггінгу)

.NET-framework необхідний задля реалізації зручного користувацького інтерфейсу та обробки подій (натискання та віджимання клавіш).

Мова C++ містить мінімально необхідний функціонал задля реалізації математичного апарату засобів в зручному для демонстрації віконному інтерфейсі.

3.2 Розробка блок-схем алгоритмів роботи

Блок-схеми роботи модулів засобів наведено далі на рисунках 3.1 – 3.4.

Рисунок 3.1 – Блок-схема узагальненого алгоритму роботи модулю обрання режиму подальшої взаємодії з засобами

Блок 2 – створюється директорія бази даних;

Блок 3 – користувач вводить свій логін;

Блок 4 – користувач обирає бажаний режим роботи;

Блок 5 – після завершення роботи в будь-якому режимі, користувач може завершити або продовжити свою роботу з засобами.

Рисунок 3.2 – Блок-схема узагальненого алгоритму роботи модулю створення еталону заявленого користувача

Блок 2 – користувач натискає клавішу під час введення тексту, фіксується час натискання клавіши;

Блок 3 – обчислюються характеристики інтервалу часу між натисканням двох клавіш;

Блок 4 – користувач віджимає клавішу під час введення тексту, фіксується час віджимання клавіши;

Блок 5 – обчислюються характеристики часу утримання клавіши;

Блок 6 – користувач може продовжити введення тексту або зберегти еталон;

Блок 7 – еталон зберігається в поточній директорії користувача;

Блок 8 – користувач може продовжити роботу в режимі створення еталону або завершити його та вийти в головне меню.

Рисунок 3.3 – Блок-схема узагальненого алгоритму роботи модулю аутентифікації користувача

Блок 2 – користувач натискає клавішу під час введення тексту, фіксується час натискання клавіши;

Блок 3 – обчислюються характеристики інтервалу часу між натисканням двох клавіш;

Блок 4 – користувач віджимає клавішу під час введення тексту, фіксується час віджимання клавіши;

Блок 5 – обчислюються характеристики часу утримання клавіши;

Блок 6 – користувач може продовжити введення тексту або спробувати аутентифікуватися;

Блок 7 – з бази даних зчитуються еталонні характеристики заявленого користувача;

Блок 8 – зчитані еталоні характеристики зіставляються з поточними;

Блок 9 – виводиться результат аутентифікації;

Блок 10 – користувач може продовжити роботу в режимі аутентифікації або завершити його та вийти в головне меню.

Рисунок 3.4 – Блок-схема узагальненого алгоритму роботи модулю ідентифікації користувача

Блок 2 – користувач натискає клавішу під час введення тексту, фіксується час натискання клавіши;

Блок 3 – обчислюються характеристики часу інтервалу між натисканням двох клавіш;

Блок 4 – користувач віджимає клавішу під час введення тексту, фіксується час віджимання клавіши;

Блок 5 – обчислюються характеристики часу утримання клавіши;

Блок 6 – користувач може продовжити введення тексту або спробувати ідентифікуватися;

Блок 7 – перебір всіх існуючих директорій в директорії бази даних;

Блок 8 – зчитані еталоні характеристики зіставляються з поточними;

Блок 9 – виводиться результат ідентифікації;

Блок 10 – користувач може продовжити роботу в режимі ідентифікації або завершити його та вийти в головне меню.

3.3 Розробка модулів програмного забезпечення

3.3.1 Модуль обрання режиму роботи

Головний модуль обрання режиму роботи містить поле вводу логіна користувача, що необхідно задля створення відповідної директорії в базі даних а також однойменні кнопки для переходу в режими створення еталону, аутентифікації або ідентифікації.

В модулі активно використовується бібліотека direct.h – яка спрощує маніпуляції з файловою системою (зміна активної директорії, створення нової директорії).

Вихідний код модулю обрання режиму наведено в додатку Б.

3.3.2 Модуль створення еталону

Модуль створення еталону містить поле для введення тексту, два текстових поля для відображення вихідних даних (час утримання клавіши, інтервал часу

між натисканням клавіш), які будуть використовуватися для обчислення характеристик, та дві кнопки – «Збереження еталону» і «Вихід».

В модулі активно використовуються такі бібліотеки:

cmath – спрощує реалізацію математичного апарату засобів, було використано деякі функції з бібліотеки (pow – для підведення до степеню та sqrt – для обчислення кореню).

fstream – необхідна для збереження характеристик в базі даних у вигляді текстових файлів з розширенням txt.

time.h – спрощує операції з системним часом, що дозволяє легко фіксувати час натискання та віджимання клавіш.

filesystem – стандартна бібліотека для маніпуляцій з файловою системою, більш оптимізована і зручна ніж direct.h саме для зміни директорії.

В таблиці 3.1 наведено опис змінних, що використовуються для реалізації алгоритму створення еталону. Повний вихідний код модулю наведено в додатку В.

Таблиця 3.1 – Опис змінних, використаних в модулі створення еталону

Тип змінної	Ім’я змінної	Задане значення	Призначення
int	start	0	Фіксування часу в момент натискання клавіши
int	end	0	Фіксування часу в момент віджимання клавіши
char	symbol	0	Код поточного введеного символу
char	symbol_buf	0	Код попереднього введеного символу
array int	arr_pressing_time_counter	(94) = 0	Масив лічильників введених символів
array int	arr_pressing_time_average	(94) = 0	Масив характеристик середнього часу утримання введених символів
array int	arr_pressing_time_average_deviation	(94) = 0	Масив характеристик середнього часу відхилення введених символів
array int	arr_pressing_time_range_min_max	(94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених символів
array int	arr_pressing_interval_counter	(94, 94) = 0	Масив лічильників введених парних комбінацій символів
array int	arr_pressing_interval_average	(94, 94) = 0	Масив характеристик середнього часу утримання введених парних комбінацій символів
array int	arr_pressing_interval_average_deviation	(94, 94) = 0	Масив характеристик середнього часу відхилення введених парних комбінацій символів
array int	arr_pressing_interval_range_min_max	(94, 94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених парних комбінацій символів

3.3.3 Модуль аутентифікації

Модуль аутентифікації містить поле для введення тексту, чотири текстових поля – два для відображення границь еталону (час утримання клавіши, інтервал часу між натисканням клавіш), два для результатів аутентифікації по кожній характеристиці, а також повзунок для регуляції коефіцієнту дозволеного допуску.

В модулі активно використовуються ті самі бібліотеки, що й в модулі створення еталону.

В таблиці 3.2 наведено опис змінних, що використовуються для реалізації алгоритму аутентифікації. Повний вихідний код модулю наведено в додатку Г.

Таблиця 3.2 – Опис змінних, використаних в модулі аутентифікації

Тип змінної	Ім’я змінної	Задане значення	Призначення
int	start	0	Фіксування часу в момент натискання клавіши
int	end	0	Фіксування часу в момент віджимання клавіши
char	symbol	0	Код поточного введеного символу
char	symbol_buf	0	Код попереднього введеного символу
array int	arr_pressing_time_counter	(94) = 0	Масив лічильників введених символів
array int	arr_pressing_time_average	(94) = 0	Масив характеристик середнього часу утримання введених символів
array int	arr_pressing_time_range_min_max	(94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених символів еталону
array int	arr_pressing_interval_counter	(94, 94) = 0	Масив лічильників введених парних комбінацій символів
array int	arr_pressing_interval_average	(94, 94) = 0	Масив характеристик середнього часу утримання введених парних комбінацій символів
array int	arr_pressing_interval_range_min_max	(94, 94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених парних комбінацій символів еталону

3.3.4 Модуль ідентифікації

Модуль ідентифікації містить поле для введення тексту, два текстових поля (час утримання клавіши, інтервал часу між натисканням клавіш), в яких містяться результати ідентифікації по кожній характеристиці кожного користувача в базі даних.

В модулі активно використовуються ті самі бібліотеки, що й в модулі створення еталону.

В таблиці 3.3 наведено опис змінних, що використовуються для реалізації алгоритму аутентифікації. Повний вихідний код модулю наведено в додатку Д.

Таблиця 3.3 – Опис змінних, використаних в модулі ідентифікації

Тип змінної	Ім’я змінної	Задане значення	Призначення
int	start	0	Фіксування часу в момент натискання клавіши
int	end	0	Фіксування часу в момент віджимання клавіши
int	counter_positive_result	0	Лічильник влучень в межі еталону
char	symbol	0	Код поточного введеного символу
char	symbol_buf	0	Код попереднього введеного символу
array int	arr_pressing_time_counter	(94) = 0	Масив лічильників введених символів
array int	arr_pressing_time_average	(94) = 0	Масив характеристик середнього часу утримання введених символів
array int	arr_pressing_time_range_min_max	(94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених символів еталону
array int	arr_pressing_interval_counter	(94, 94) = 0	Масив лічильників введених парних комбінацій символів
array int	arr_pressing_interval_average	(94, 94) = 0	Масив характеристик середнього часу утримання введених парних комбінацій символів
array int	arr_pressing_interval_range_min_max	(94, 94, 2) = 0	Масив характеристик нижньої та верхньої границі часу відхилення введених парних комбінацій символів еталону

3.4 Перевірка працездатності програмного забезпечення

3.4.1 Меню обрання режиму

Модуль обрання режиму роботи повинен виконувати наступні функції:

– створювати директорію бази даних
– створювати директорію заявленого користувача за його логіном
– попереджати про недопустимість аутентифікації за пустим логіном
– попереджати про те, що заявленого користувача не знайдено в базі

Перевірка працездатності всіх функцій наведена далі на рисунках 3.5 – 3.9

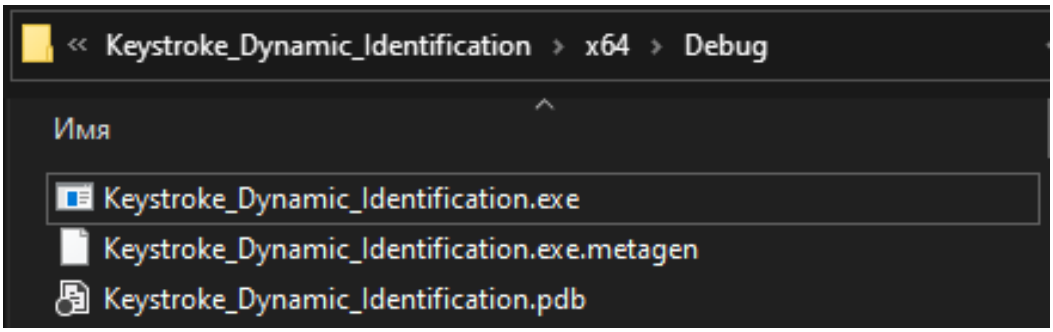


Рисунок 3.5 – Директорія програмного засобу до запуску програми

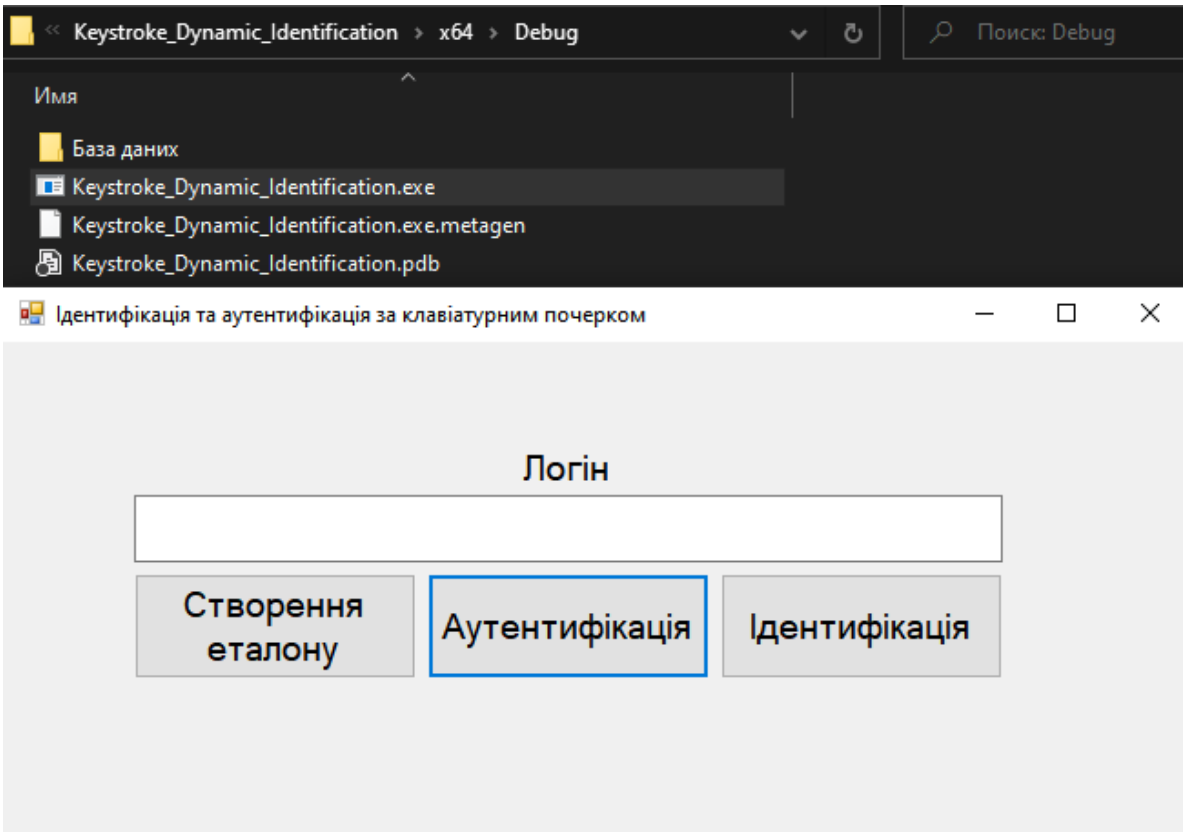


Рисунок 3.6 – Директорія програмного засобу після запуску програми

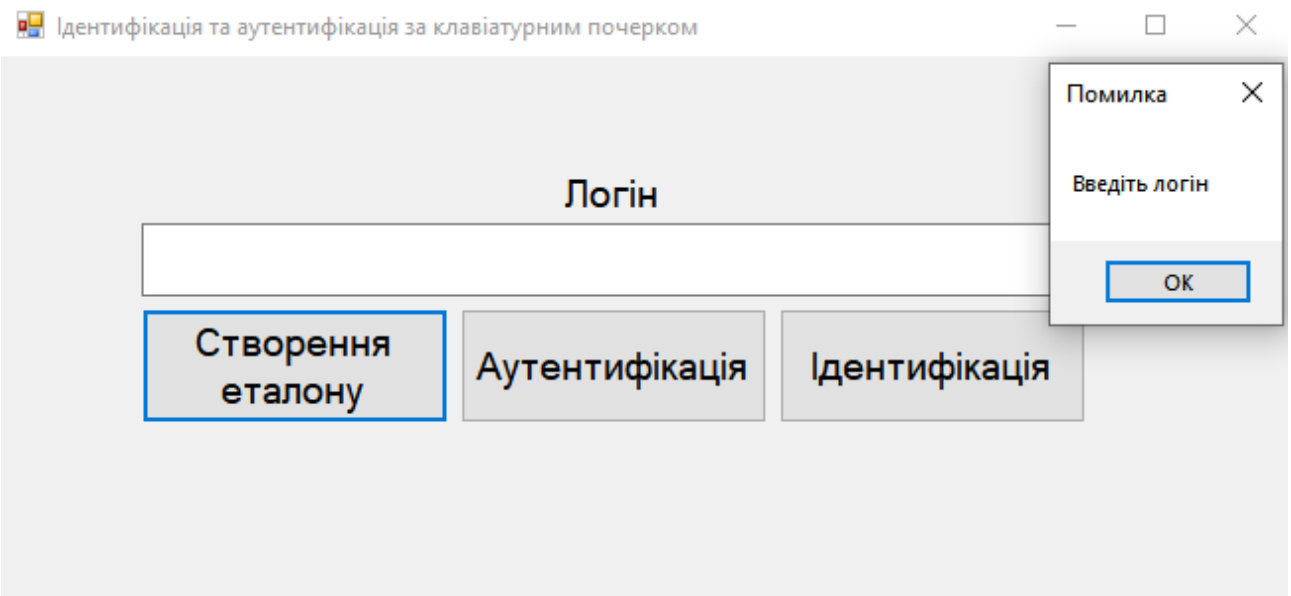


Рисунок 3.7 – Спроба обрати режим створення еталону або аутентифікації без введення логіну

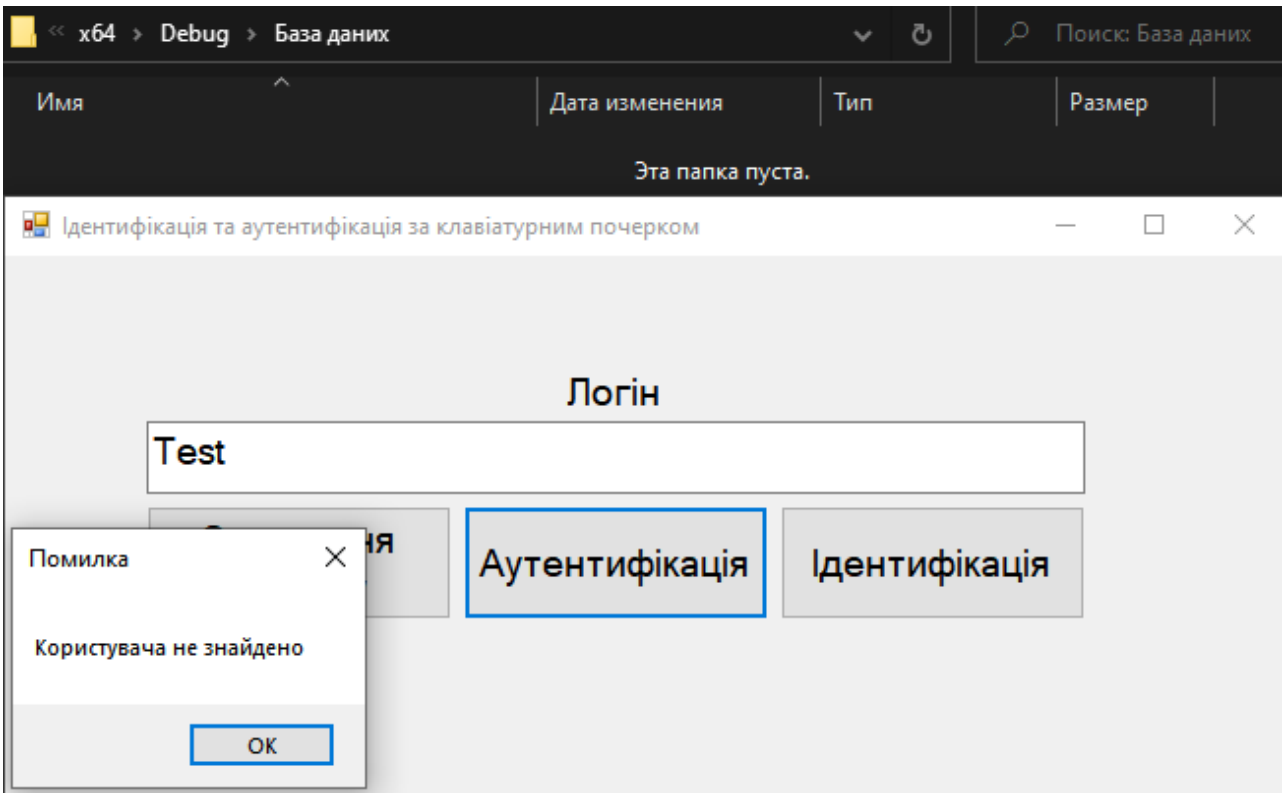


Рисунок 3.8 – Спроба пройти аутентифікацію за відсутнім у базі даних логіном

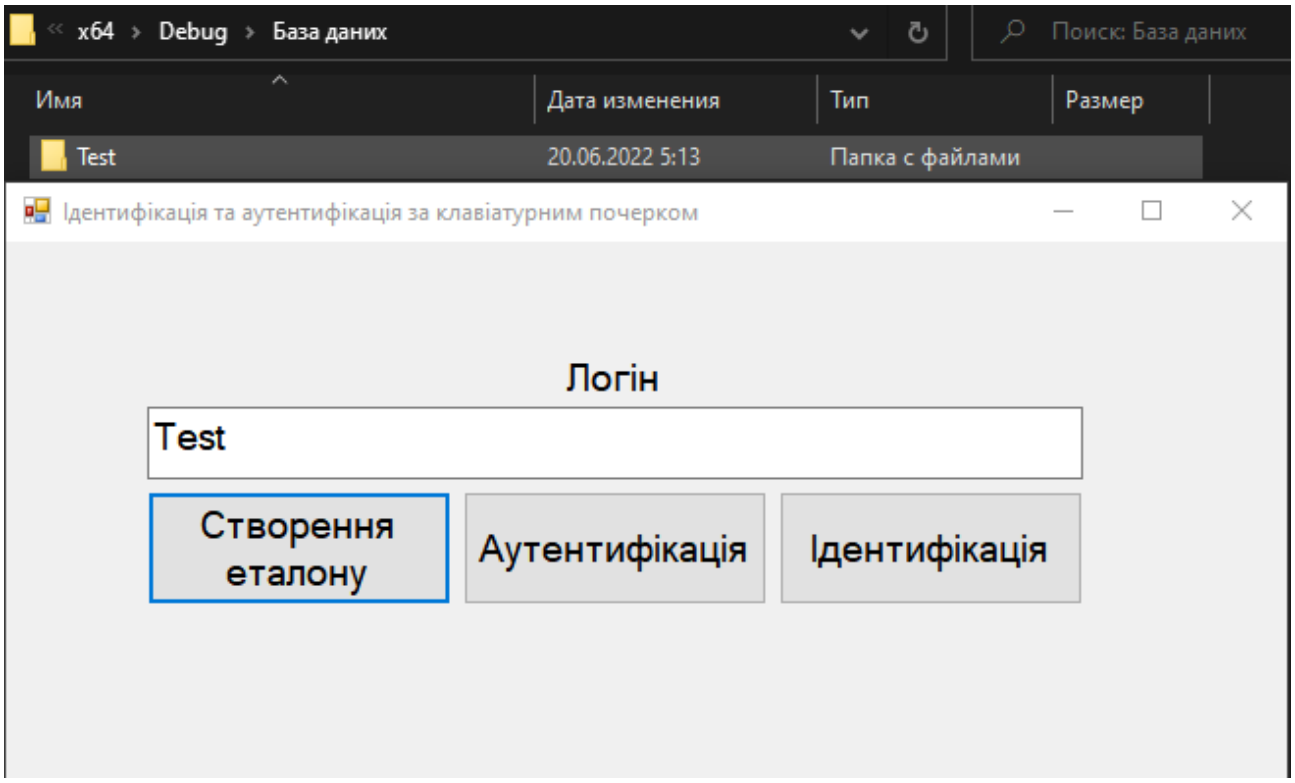


Рисунок 3.9 – Створення директорії заявленого користувача в базі даних

3.4.2 Режим створення еталону

Модуль створення еталону повинен виконувати наступні функції:

– відображати вихідні дані у текстових полях
– зберігати еталон у відповідних текстових файлах

Перевірка працездатності всіх функцій наведена далі на рисунках 3.10 – 3.13

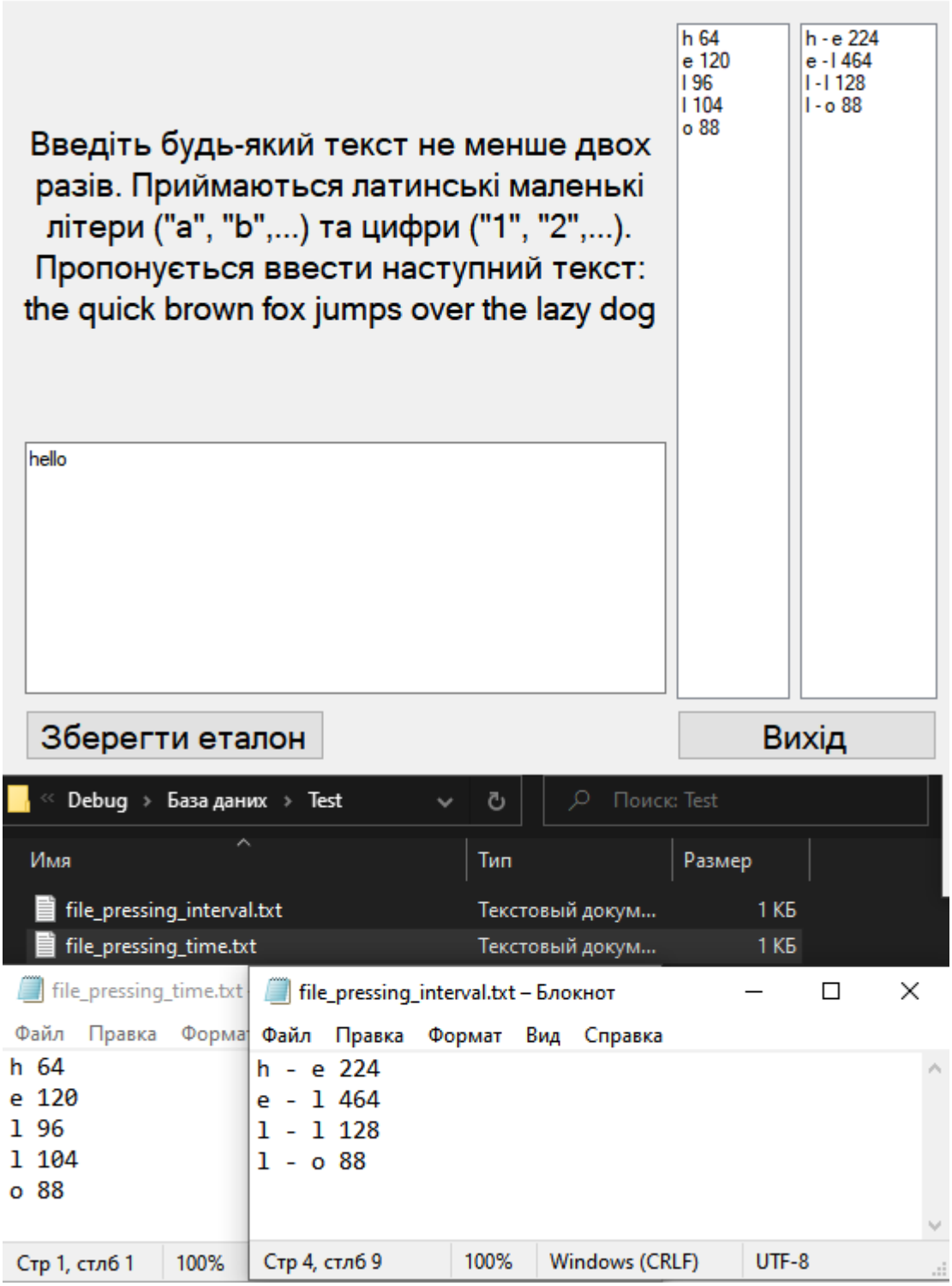


Рисунок 3.10 – Вигляд директорії користувача до збереження еталону

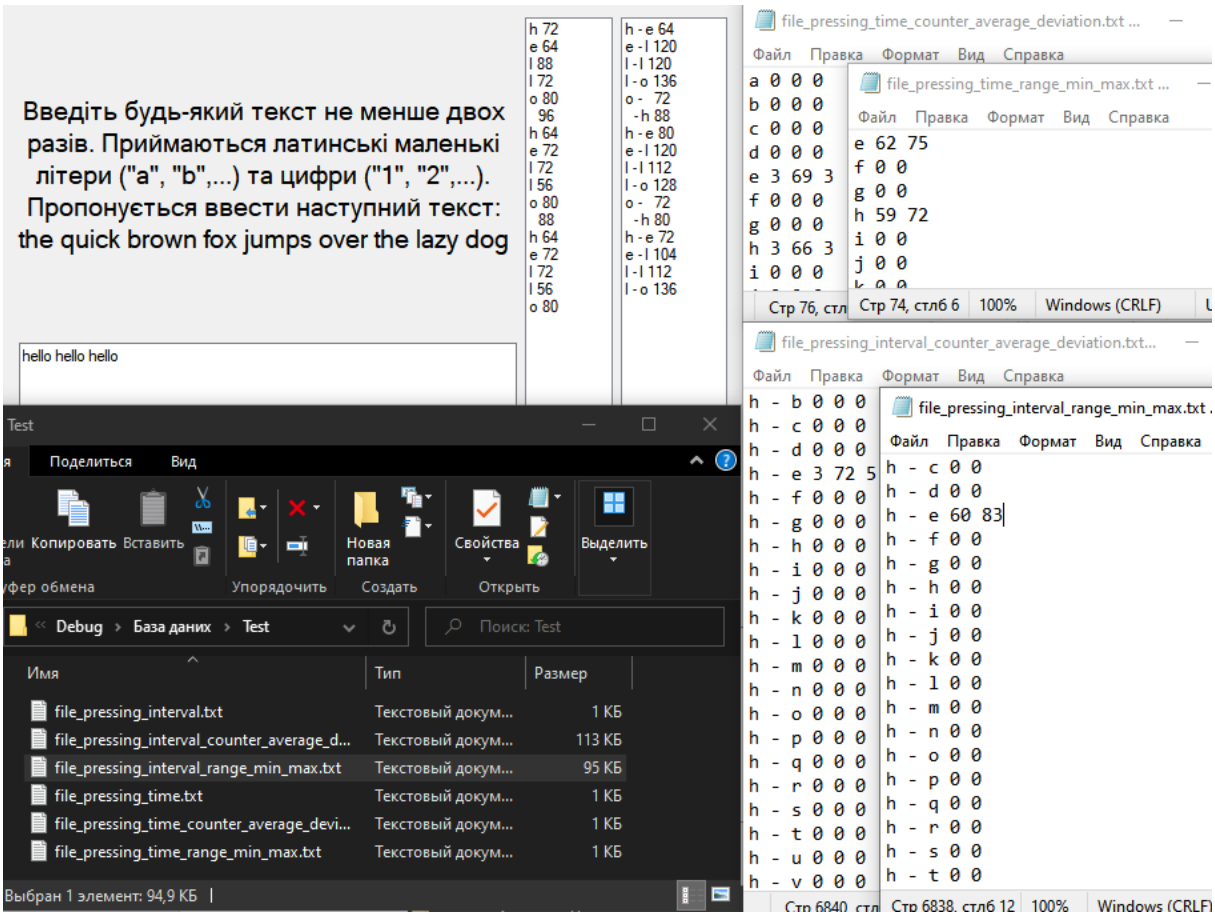


Рисунок 3.11 – Вигляд директорії користувача після збереження еталону

3.4.3 Режим аутентифікації

Модуль аутентифікації повинен виконувати наступні функції:

– завантажувати еталонні характеристики заявленого користувача з бази даних
– виводити результати зіставлення поточних характеристик з еталонними
– змінювати коефіцієнт допуску з метою демонстрації за бажанням користувача
– виводити результат спроби аутентифікації

Перевірка працездатності всіх функцій наведена далі на рисунках 3.12 – 3.13

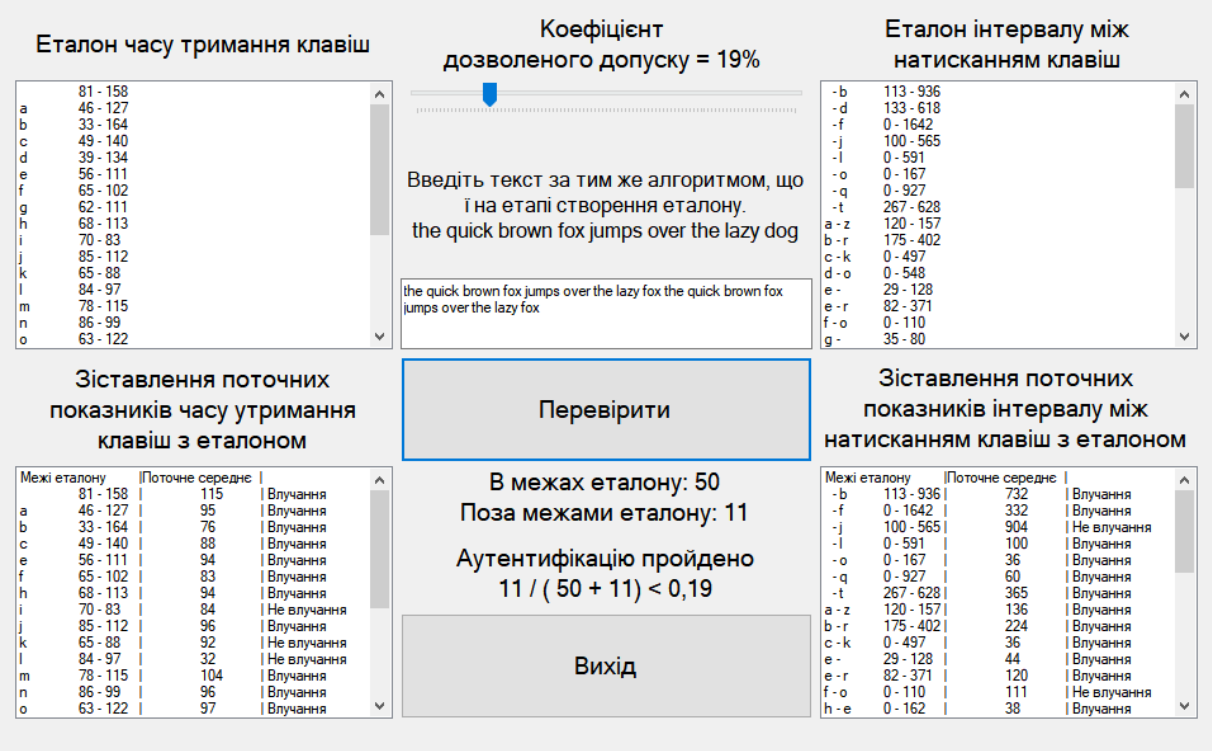


Рисунок 3.12 – Приклад вдалої аутентифікації

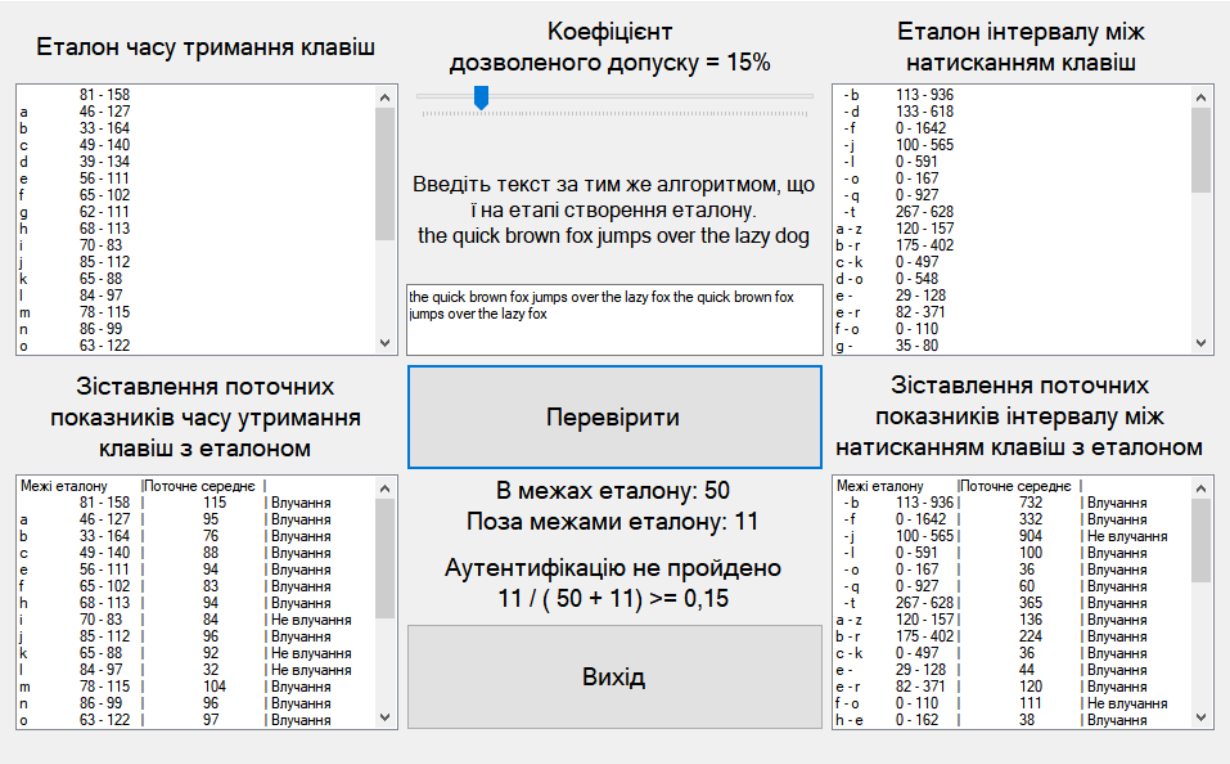


Рисунок 3.13 – Приклад невдалої аутентифікації після зміни коефіцієнту

3.4.4 Режим ідентифікації

Модуль ідентифікації повинен виконувати наступні функції:

– завантажувати з бази даних еталонні характеристики користувачів
– виводити результати зіставлення поточних характеристик з еталонними
– виводити результат спроби ідентифікації

Перевірка працездатності всіх функцій наведена далі на рисунку 3.14.

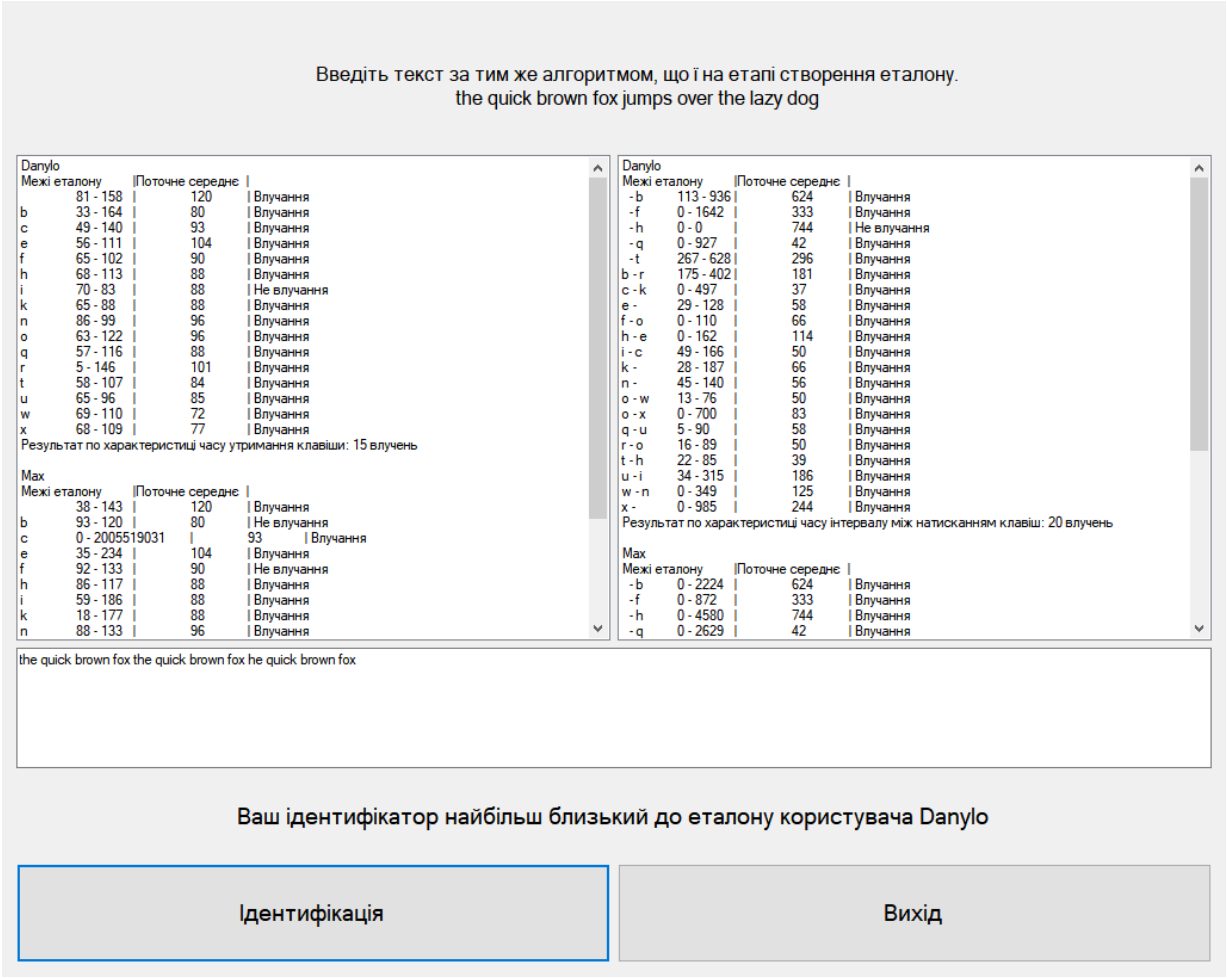
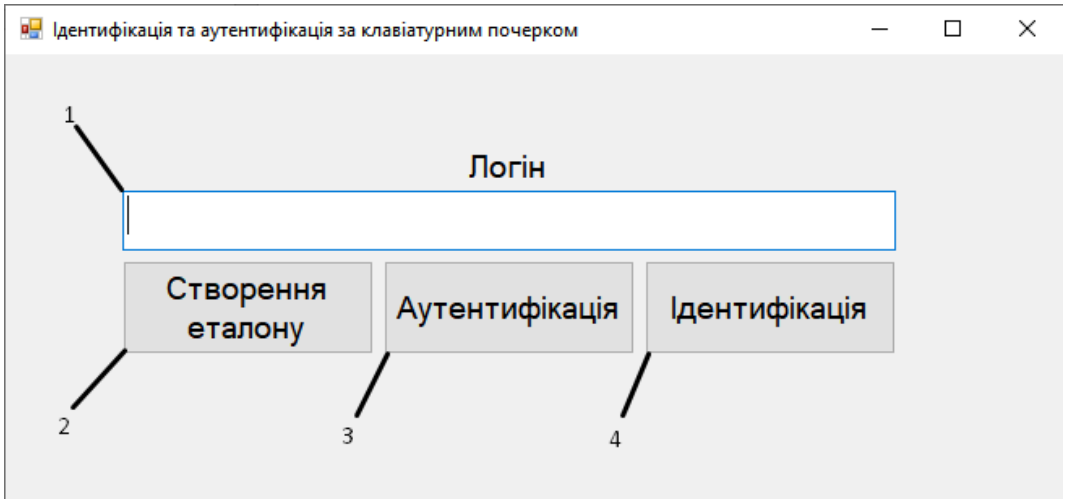


Рисунок 3.14 – Результати ідентифікації

3.5 Інструкція з використання засобів

Призначення елементів засобів у відповідних режимах наведено на рисунках 3.15 – 3.18.



поле вводу логіну (1); кнопка переходу в режим створення еталону (2); кнопка переходу в режим аутентифікації (3); кнопка переходу в режим ідентифікації (4)

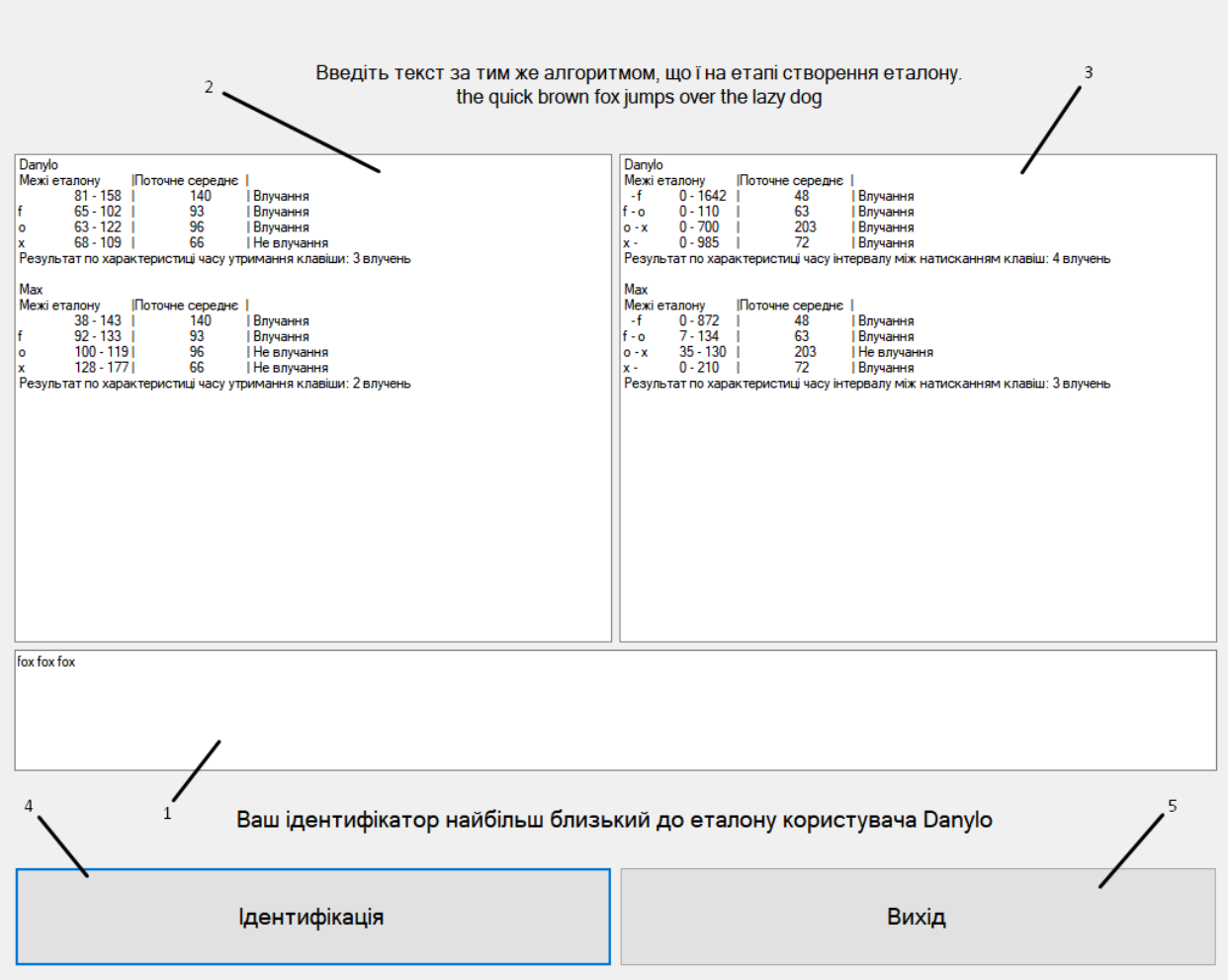
Рисунок 3.15 – Вікно головного меню

поле введення тексту (1); відображення вихідних даних часу утримання клавіш (2); відображення вихідних даних інтервалу між натисканням клавіш (3); кнопка збереження еталону (4); кнопка виходу в головне меню (5);

Рисунок 3.16 – Вікно режиму створення еталону

поле введення тексту (1); повзунок зміни коефіцієнту дозволеного допуску (2); кнопка для спроби аутентифікації (3); відображення еталонних характеристик користувача (4, 5); відображення зіставлення поточних характеристик з еталонними (6, 7); кнопка виходу в головне меню (8)

Рисунок 3.17 – Вікно режиму аутентифікації



поле введення тексту (1); зіставлення поточних характеристик з еталонними (2, 3); кнопка для спроби ідентифікації (4); кнопка виходу в головне меню (5)

Рисунок 3.18 – Вікно режиму ідентифікації

3.6 Висновки за розділом

Обрані засоби реалізації комплексу, створені блок-схеми алгоритмів роботи модулів окремих режимів. На основі блок-схем розроблено програмне забезпечення демонстрації ідентифікації та аутентифікації, протестовані їх функції. Створена інструкція з використання засобів.

ВИСНОВКИ

Розроблено програмні засоби для демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком під час введення текстового фрагменту.

В кваліфікаційній роботі розглянуто та проаналізовано біометричні методи аутентифікації, алгоритми розпізнавання за клавіатурним почерком.

Представлено схему функціонування прототипів засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком та їх математична модель.

Створені блок-схеми алгоритмів роботи модулів окремих режимів. На основі блок-схем, за допомогою обраних засобів реалізації комплексу, розроблено засоби демонстрації аутентифікації та ідентифікації за клавіатурним почерком, протестовані їх функції. Створена інструкція з використання засобів. Розроблені засоби можуть бути використані в навчальних цілях при виконанні лабораторних робіт студентами в рамках відповідних дисциплін.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке багатофакторна аутентифікація (MFA) [Електрон.ресурс] – Режим доступу: https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya

2. Закон України Про електронні довірчі послуги [Електрон.ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n104

3. Захаров, В. П. Біометричні технології в XXI столітті та їх використання правоохоронними органами [Текст] : посібник / В. П. Захаров, В. І. Рудешко. – 2-ге вид., доп. – Львів: ЛьвДУВС, 2015. – 492 с.

4. Бідюк, П. Сучасні методи біометричної ідентифікації [Текст] / П. Бідюк, В. Бондарчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2009. – Вип. 1(18). – С. 137-146.

5. Yevetskyi, V. Analysis of stability of the user's keyboard handwriting characteristics in the biometric authentication systems / V. Yevetskyi, I. Horniichuk // Information Technology and Security. – 2018. – Vol. 6, Iss. 2 (11). – Pp. 19–28.

6. Теорія імовірностей і математична статистика [Текст]. У 2 ч. Ч. І. Теорія ймовірностей / В. І. Жлуктенко, С.І. Наконечний; за ред. О.П. Бондаренко. – К.: КНЕУ, 2000. – 304 с.

7. ISO/IEC 14882 Fifth edition 2017-12 [Електроний рисурс] / Режим доступу: https://webstore.iec.ch/preview/info_isoiec14882%7Bed5.0%7Den.pdf